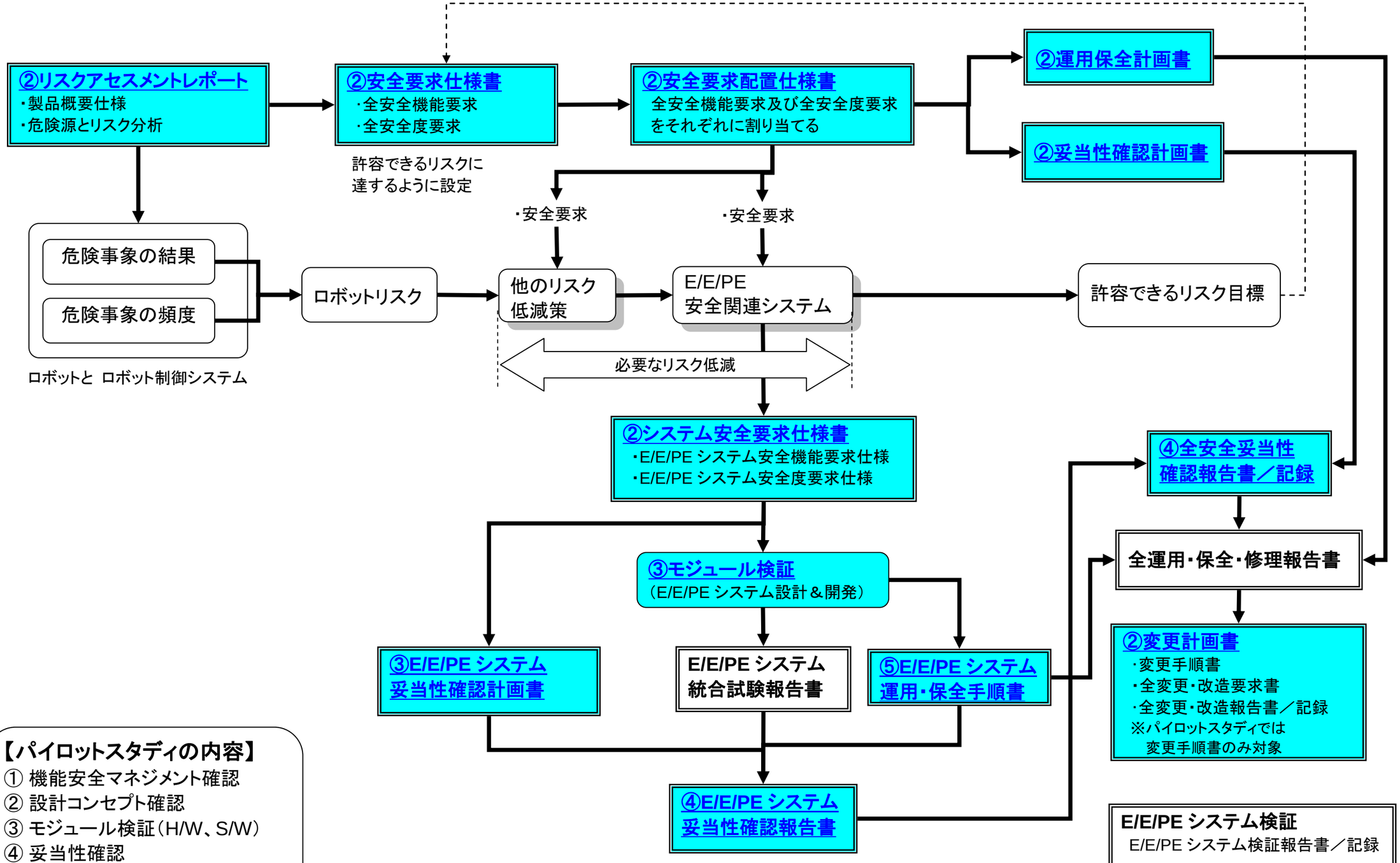


【パイロットスタディの内容】

① 機能安全マネジメント確認
② 設計コンセプト確認
③ モジュール検証（H/W、S/W）
④ 妥当性確認
⑤ 文書確認

：パイロットスタディで確認させていただく部分

リスクアセスメントレポート（製品概要仕様を含む）

※リスクアセスメントのひな型シートなどを参照

項番	内容	備考
1-1	・ロボットの概要仕様 ・ロボットとその制御機能の概要 ・ロボットの意図した使用	合理的に予見できる誤使用や物理的な使用空間や制限などを含む
1-2	同定した危険源に関する情報	・ヒューマンファクターや他の機器との相互作用による危険源、危険状態および危険事象なども考慮
1-3	リスク見積り	リスク基準値（危害の酷さ及び危害の発生確率）などが明確なこと
1-4	リスク評価	許容できるリスク、リスク低減の必要性などの基準値などが明確なこと

安全要求仕様書

安全機能要求と安全度要求に関する全安全要求仕様書

項番	参照項番	内容	備考
2-1	7.5.2.1 7.5.2.3	・危険源とリスク分析から導き出せる全安全機能および各全安全機能に関する目標安全度要求 ・許容できるリスク値とその考え方（方針）	・全安全機能は、危険源とリスク分析から導き出される危険事象に基づいていること ・全安全機能が許容できるリスクの範囲であることが分かること ・全安全機能の例； 駆動スピードは 3,000 rpm を超えないようにするなど
2-2	7.5.2.4	全安全度要求（次のいずれかで規定） ① 許容できるリスクを達成するために要求されるリスク低減方策 (consequence of the hazardous event) ② 許容できるリスクを達成するために要求される危険事象率の低減方策 (frequency of the hazardous event)	全安全度要求の例； ① 駆動スピードが 3,000 rpm を超えないように、かつ、それが許容できるリスクであるようにするには、どのようにおよびどの程度リスク低減するかなど ② 駆動スピードが 3,000 rpm を超える事象の発生率を許容できるレベルであるようにするには、どの程度危険事象の発生率を低減するかなど

例示

危険源および危険事象 （リスク分析の結果からの導きだされたもの）	全安全機能 （安全機能の内容が許容できるリスクに達するものであること）	目標安全度要求／全安全度要求 （危険事象の結果を軽減するのか、または危険事象の発生率を軽減するのか。そしてそれらが許容できるリスクに達成するものであるかどうか）
駆動スピードが 3,000 rpm を超えると、ロボットの周りの人が、ロボットを避けることができず、（医療措置が必要な）怪我を負う	駆動スピードは 3,000 rpm を超えないようにする	駆動スピードが 3,000 rpm を超える事象の発生率を〇〇まで下げる （この措置が許容できるリスクを達成すること）

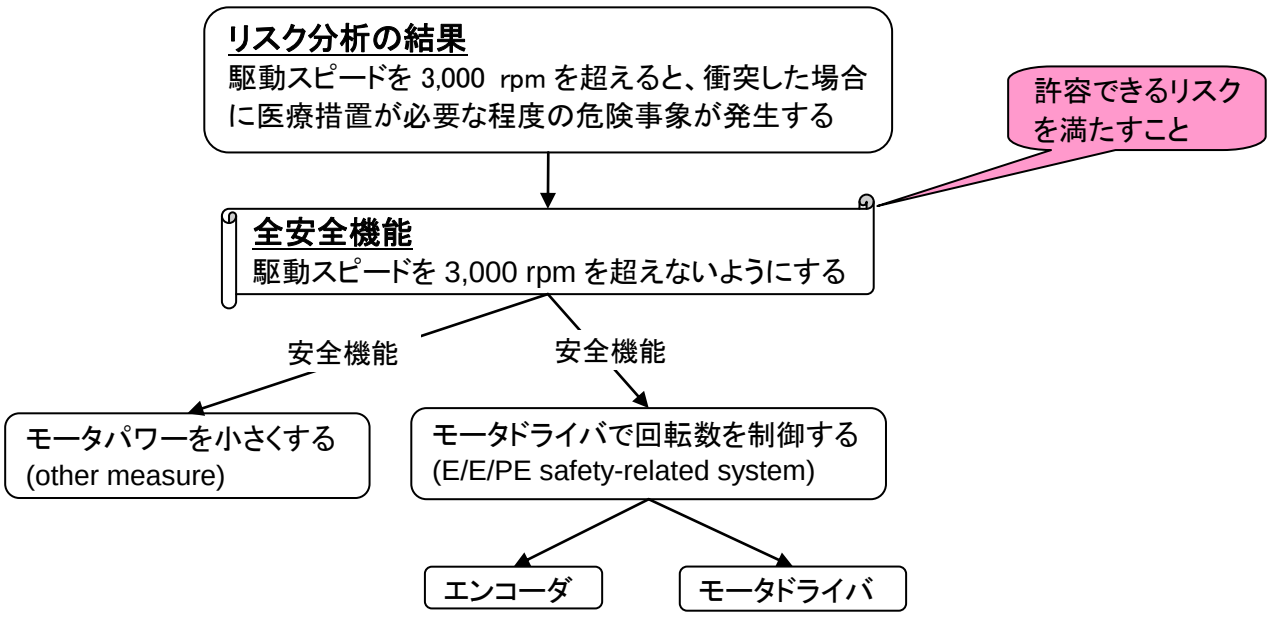
安全要求配置仕様書

E/E/PE 安全関連システムや他のリスク低減策に割り当てた安全要求

項番	参照項番	内容	備考
3-1	7.6.2.1	要求される機能安全を達成するために用いる安全関連システムを指定	ブロック図や回路図などで示しても可
3-2	7.6.2.4 7.6.2.5	E/E/PE 安全関連システムおよび／または他のリスク低減策に割り当てた安全要求	
3-3	7.6.2.4	割り当てた各安全機能に対する目標機能失敗尺度（target failure measure） →PFD または PFH で規定される安全度要求について達成される危険モード故障の目標確率	低頻度作動要求モードでは作動要求当たりに機能の実行を失敗する平均確率で、高頻度作動要求または連続モードでは時間当たりの危険側機能失敗確率で定める
3-4	7.6.2.7	E/E/PE 安全関連システムおよび他のリスク低減策を独立したものをして扱うかどうか。 独立したものをして扱う場合は、次についてどのように対応しているかなど （共通原因故障を考慮しているか） ・異なるシステム又は方策間において故障が同時に起こる可能性 ・機能的な多様性 ・技術の多様性	・E/E/PE 安全関連システムと他のリスク低減策が関連するか、又は関連しないかを示せること。（独立性） ・全てのシステムの故障について危険モードになるかもしれない部品を使用していないことが示せること ・技術の多様性については、安全度が高く、飛行機衝突や地震などシビアな結果になる危険事象で、共通原因の可能性が低いものに対する特別な予防策で認められる

例示

危険源および危険事象 （リスク分析の結果からの導きだされたもの）	全安全機能 （安全機能の内容が許容できるリスクに達するものであることが必要）	全安全度要求 （危険事象の結果を軽減するのか、または危険事象の発生率を軽減するのか。そしてそれらが許容できるリスクに達成するものであるかどうか）
駆動スピードが 3,000 rpm を超えると、ロボットの周りの人が、ロボットを避けることができず、医療措置が必要な程度の怪我を負う	駆動スピードは 3,000 rpm を超えないようにする	駆動スピードが 3,000 rpm を超える事象の発生率を〇〇まで下げる



運用保全計画書

メンテナンス手順

項番	参照項番	内容	備考
4-1	7.7.2.1	・E/E/PE 安全関連システムの機能安全を維持するために必要な通常の活動（routine action） ・安全でない状態の防止、E/E/PE 安全関連システムへの作動要求の軽減、または危険事象による被害を軽減するために必要な業務と制限 ・保管しなければならない文書（機能安全監査結果、テスト結果やインシデント情報など） ・メンテナンスの範囲 ・危険事象が起きた場合に取るべき措置 ・オペレーションとメンテナンスの記録（時系列）	
4-2	7.7.2.2	・E/E/PE 安全関連システムのサブシステムのハードウェアトレランス（HT）がゼロ又はゼロより大きい場合のロボットの安全の維持を確実にするための方法	HT がゼロのサブシステムが試験のためオフラインにしなければならない場合、どのようにロボットの安全を維持するか。 HT がゼロより大きいサブシステムの場合、最低 1 チャンネルが試験中に動作し続け、MTTR 内に完了すること
4-3	7.7.2.3	潜在故障の発見活動	
4-4	7.7.2.4	オペレーションとメンテナンスの責任者による E/E/PE 安全関連システムの維持のための計画の合意文書	

妥当性確認計画書

項番	参照項番	内容	備考
5-1	7.8.2.1	全安全機能のうち、どのようなタイミングで、どのような安全機能の妥当性確認を実施するのか	E/E/PE 安全関連システムや他のリスク低減策に割り当てられた安全機能の妥当性確認のタイミングと内容
5-2	7.8.2.1	上述の妥当性確認のため、どのような部署で、どのような試験や分析を実施するのか	
5-3	7.8.2.1	妥当性確認のために必要な環境 ・温湿度などの物理的な環境条件 ・妥当性確認に必要な機器や装置 ・妥当性確認に必要な E/E/PE 安全関連システムの仕様 ・妥当性確認に必要な動作条件（オペレーションモード）とコンフィグレーション	機器や装置については、校正の必要性（レベル）についても言及のこと
5-4	7.8.2.1	安全機能が正しく実行されていることを確認するための手順など	全安全要求仕様書で定義した全安全機能及び全安全度要求に適合していることをどのように確認するのかを含む
5-5	7.8.2.1	合否の基準	
5-6	7.8.2.1	妥当性確認の結果の評価方針と手順（特に不合格の場合）	特に不合格であった場合、どのような措置をとるのかを含む

システム安全要求仕様書

E/E/PE システム安全機能要求仕様と E/E/PE システム安全度要求仕様で構成

項番	参照項番	内容	備考
6-1	7.10.2.6	E/E/PE システム安全機能要求仕様 a) 要求される機能安全を達成するために必要な全ての安全機能の説明 b) 安全機能が完了するために必要な時間（タイミングチャートなど） c) 要求する E/E/PE 安全関連システムとオペレータインタフェース d) E/E/PE 安全関連システムの設計に影響するかもしれない、関連する機能安全の全ての情報 e) 機能安全に必要な全てのインタフェース f) ロボットの全ての関連するオペレーションモード（自動、マニュアル、リセット、メンテナンスなど） g) E/E/PE 安全関連システムの故障時の動作と要求されるレスポンス	・明確で、正確で、あいまいでなく、検証でき、テストでき、維持でき、実行可能であること ・安全状態（safe state）はどのような状態かを定義 ⇒危険故障検出における挙動として安全状態の達成結果として規定 ・安全状態（safe state）を達成・維持するためのアクションを規定
6-2	7.10.2.7	E/E/PE システム安全度要求仕様 a) 安全機能に対する安全度レベル b) 安全機能のオペレーションモード（低・高需要または連続） c) デューティーサイクルと耐用期間 d) プルーフテストに対する要求事項、制約、機能および設備 e) ライフサイクルの間で直面しそうな極端な環境条件 f) 電磁イミュニティの限度値 g) 共通原因故障の可能性による E/E/PE 安全関連システムの実現のための制限および制約	

変更計画書

手順書、要求書及び報告書から構成

変更・改造手順書

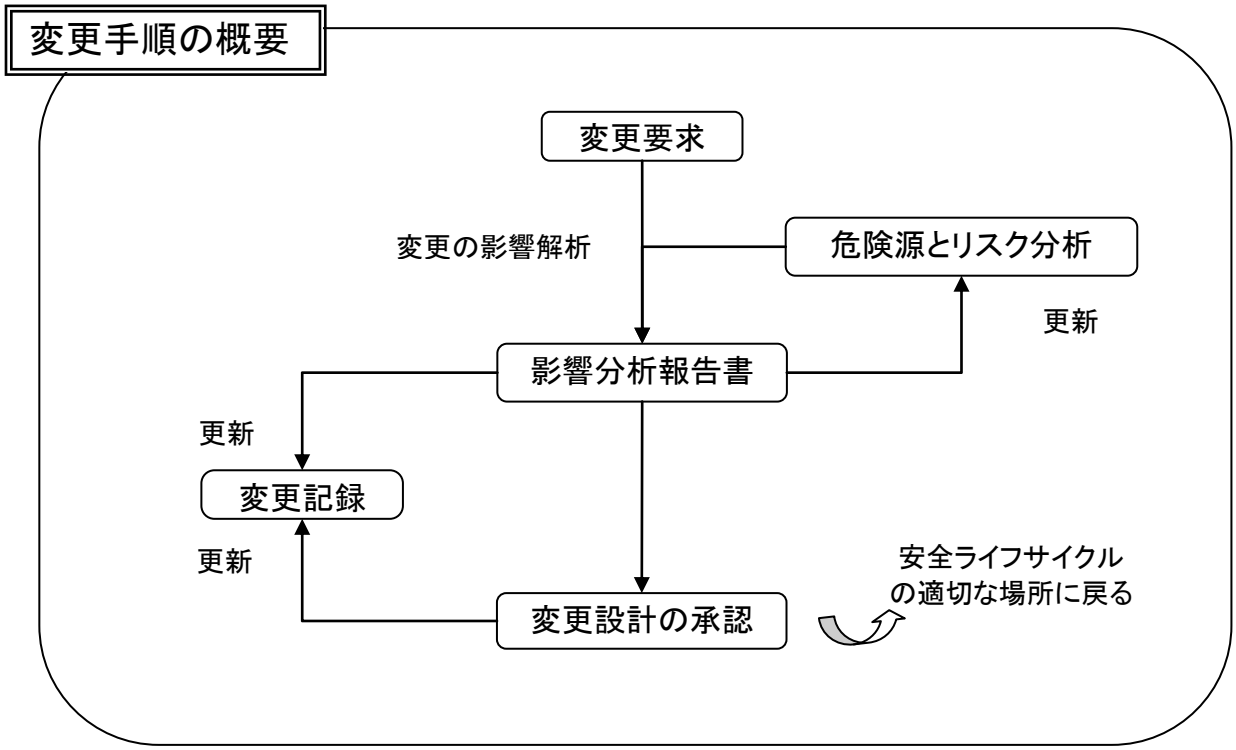
項番	参照項番	内容	備考
7-1-1	7.16.2.1 7.16.2.5 7.16.2.6	・E/E/PE 安全関連システムの変更・改造を開始する手順 ・変更・改造の承認と権限の取得手順	・変更・改造は、変更・改造の承認と権限を得た上で、開始されること ・要求された変更・改造の実施の承認は、影響分析の結果に基づくものであること ・E/E/PE 安全関連システムの機能安全に影響する全ての変更・改造は、ライフサイクルの適切なフェーズに戻って開始しなければならない

全変更・改造要求書

項番	参照項番	内容	備考
7-2-1	7.16.2.2	- 影響を受ける可能性がある同定された危険源 - 提案された変更内容 - 変更の理由	
7-2-2	7.16.2.3	影響解析の結果	提案された変更内容の影響評価を含む

全変更・改造報告書／記録

項番	参照項番	内容	備考
7-3-1	7.16.2.7	- 修正または改造の要求書 - 影響分析報告書 - データの再検証と再妥当性確認および結果 - 修正と改造によって影響を受ける全ての文書	変更／改造の開始には責任者による正式な承認が必要



モジュール検証（E/E/PE システム設計＆開発）で必要となる資料

① 故障解析レポート
② システムブロック図
③ ハードウェア仕様書
④ モジュール仕様書
⑤ 回路図
⑥ 部品表
⑦ コーディング規約
⑧ ソフトウェア構造仕様書
⑨ ソフトウェア安全仕様書
⑩ ソフトウェアモジュール仕様書
⑪ ソースコードリスト

E/E/PE システム妥当性確認計画書

項番	参照項番	内容	備考
8-1	7.3.2.2	E/E/PE システム安全要求仕様書と E/E/PE システム設計要求仕様書で定義された全ての要求事項	
8-2	7.3.2.2	安全機能が正しく実行されることを確認するために適用する手順と合否基準	安全機能ごと
8-3	7.3.2.2	要求される安全度であることを確認するために適用する手順と合否基準	安全機能ごと
8-4	7.3.2.2	妥当性確認のために必要な環境等 ・必要なツールと機器 ・評価手順 ・温湿度などの物理的な環境条件 ・動作条件やコンフィグレーション	
8-5	7.3.2.2	電磁イミュニティの確認のためのテスト手順と性能基準	
8-6	7.3.2.2	妥当性確認の失敗を解決するためのポリシー	

E/E/PE システム妥当性確認報告書

項番	参照項番	内容	備考
10.6-1	7.7.2.4	E/E/PE システム安全妥当性確認計画書のバージョン	
10.6-2	7.7.2.4	テスト（または解析）対象の安全機能	
10.6-3	7.7.2.4	妥当性確認に使用したツールと機器	校正データを含む
10.6-4	7.7.2.4	各テスト結果	
10.6.-5	7.7.2.4	予想した結果と実際の結果との不一致	・予想した結果と実際の結果との比較 ・どのように、どれくらい不一致があったか など
10.6-6	7.7.2.5	10.6-5 で不一致があった場合、どのような解析をしたか、また、どのような対応を取るか。	とるべき対応は、妥当性確認を続行するか、変更要求を出して、妥当性試験のどの段階に戻るかなど
10.6-7	7.7.2.7	使用した技術と方策	IEC61508-2 の TableB.5 による

E/E/PE システム運用・保全手順書

項番	参照項番	内容	備考
10.5-1	7.6.2.1	・安全機能を保全するために必要なルーチン活動（エレメントの置き換えなども含む） ・安全でない状態を避けるため、及び／又は危険事象の結果を低減するために必要な活動と制約 ・E/E/PE 安全関連システムのシステム故障と要求率を維持のために必要な文書 ・E/E/PE 安全関連システムの監査とテスト結果を維持のために必要な文書 ・E/E/PE 安全関連システムで障害や故障が起こったときにフォローする保全手順（次を含む） - 障害診断と修繕手順 - 妥当性の再確認の手順 - 保全報告に必要な事項 - オリジナル機器アイテムが使用できないか、新しいバージョンのものになった場合の妥当性の再確認手順	メンテナンススケジュールを含む
10.5-2	7.6.2.3	安全関連エレメントで明らかにされていない故障があるものについての FMEA 結果やフォールトツリー試験結果	FMEA や FTA など
10.5-3	7.6.2.4	ロボットに与えるかもしれない影響についての評価結果	
10.5-4	7.6.2.5	使用した技術と方策	IEC61508-2 の TableB.4 による

全安全妥当性確認報告書／記録

項番	参照項番	内容	備考
13-1	7.14.2.3	妥当性確認に使用した全安全要求仕様書のバージョン	
13-2	7.14.2.3	妥当性確認した安全機能	妥当性確認の対象は何か
13-3	7.14.2.3	妥当性確認で使用した機器や装置の識別	校正データを含む
13-4	7.14.2.3	妥当性確認の結果	
13-5	7.14.2.3	テストしたアイテム、適用した手順およびテスト環境の構成の識別	
13-6	7.14.2.3	期待値と実際の結果の不整合（どのように、どれくらい不整合があったかなど）	
13-7	7.14.2.4	13-6 で不整合があった場合、どのような対応を取るか	妥当性確認を続行するか、変更要求を出すか。また、なぜそのように判断したかの理由

※「モジュール検証（E/E/PE システム設計＆開発）」の中の “ハードウェア仕様書”及び“モジュール仕様書”の参考

項番	参照項番	内容	備考
10.1-1	7.2.3.2	安全機能に関連した設計要求と安全度に関連した設計要求	・明確で、正確で、あいまいでなく、検証でき、テストでき、維持でき、実行可能であること ・E/E/PE 安全ライフサイクルのフェーズにおいて、情報を利用する可能性がある人の理解を助けるように書かれていること ・E/E/PEシステム安全要求仕様にトレースできること
10.1-2	7.2.3.2	安全機能に関するサブシステムの要求事項	必要に応じて H/W、S/W エレメントの要求事項
10.1-3	7.2.3.2	E/E/PEシステム安全機能要求仕様書を満足するためのサブシステムとそのハードウェアおよびソフトウェアの統合の要求事項	
10.1-4	7.2.3.2	応答時間の要求を満足するスループット性能	
10.1-5	7.2.3.2	測定と制御の精度と安定性の要求事項	
10.1-6	7.2.3.2	E/E/PE 安全関連システムとオペレータインタフェース	
10.1-7	7.2.3.2	E/E/PE 安全関連システムと他のシステム間のインタフェース	
10.1-8	7.2.3.2	全ての動作モード。	特に、故障動作と E/E/PE 安全関連システムの要求される応答（アラームや自動シャットダウンなど）
10.1-9	7.2.3.2	全てのハードウェア／ソフトウェアの相互作用の重要性	関係する場合は、ハードウェアとソフトウェア間の制約
10.1-10	7.2.3.2	関係するエレメントの限界と制約の条件	例えば、共通原因故障の可能性のためのタイミング制限や制約
10.1-11	7.2.3.2	スタートアップや再スタートの手順に関連した要求事項	
10.1-12	7.2.3.3	ハードウェア安全度の構造上の制約を満足するために要求する各サブシステムのアーキテクチャ	
10.1-13	7.2.3.3	目標機能失敗尺度（target failure measure）に達するために必要な、関連する信頼性モデルのパラメータ	例えば、プルーフテストの頻度のようなもの
10.1-14	7.2.3.3	診断によって危険側故障が見つかった場合にとるべき行動	
10.1-15	7.2.3.3	プルーフテストを実施するための要求事項、制約、機能および施設	
10.1-16	7.2.3.3	極端な環境状態を満足するために使用される機器の能力	E/E/PE システム安全ライフサイクルの間に要求されるものとして規定されるもの
10.1-17	7.2.3.3	電磁イミュニティレベル	
10.1-18	7.2.3.3	安全マネジメントに必要な品質保証／品質コントロール方策	IEC61508-1 の 6.2.5 項参照 ・危険源とリスク分析 ・機能安全アセスメント ・検証活動 ・コンフィグレーションマネジメント ・インシデント報告と分析 など
10.1-19	7.2.3.5	使用した技術と方策	IEC61508-2 の Table B.1 による

※「モジュール検証（E/E/PE システム設計＆開発）」の中の “ソフトウェア安全仕様書”の参考

項番	参照項番	内容	備考
10.1-1	7.2.2.3	要求される安全度を達成するための設計と実装および機能安全アセスメントを実施することができるための詳細	IEC61508-3 の Table A.1 参照
10.1-2	7.2.2.6	ロボット、E/E/PE システム及び E/E/PE システムに接続された全ての機器又はシステムの全ての関連するオペレーションモード	
10.1-3	7.2.2.7	安全関連又はハードウェアとソフトウェア間の関連する制限	
10.1-4	7.2.2.10	要求される製品の安全性特性 次のソフトウェア安全機能要求事項 1) ロボットが安全状態を達成または維持できるための機能 2) プログラマブル電子ハードウェアにおける異常検出、表示及び制御（management）に関する機能 3) センサーとアクチュエータの異常検出、表示及び制御（management）に関する機能 4) ソフトウェア自身の異常検出、表示及び制御（management）に関する機能 5) オンライン安全機能の周期的なテストに関する機能 6) オフライン安全機能の周期的なテストに関する機能 7) PE システムが安全に改修できる機能 8) 非安全関連機能へのインタフェース 9) キャパシティとレスポンス時間の性能 ソフトウェア安全度（systematic capability）の要求事項 1) 上記における各機能の安全度レベル 2) 機能間の独立性の要求事項	

※「モジュール検証（E/E/PE システム設計＆開発）」の中の “ソフトウェア構造仕様書”の参考

項番	参照項番	内容	備考
10.3-1	7.4.3.1	ソフトウェア構造設計における責任の区分	
10.3-2	7.4.3.2	a) 要求される安全度レベルにおいて、ソフトウェア安全要求仕様を満足するために必要な、選択した技術と方策の統合セットとその正当性 b) エレメント／サブシステムが既に検証されているかどうか。検証されていれば検証条件 c) 全てのソフトウェア／ハードウェア相互作用とその重要度の評価 d) 選択した全データの安全度を維持するために使用する設計機能 e) ソフトウェアアーキテクチャ統合試験	a)については IEC61508-3 の TableA.2 参照
10.3-3	7.4.3.3	E/E/PE システム安全要求仕様書の修正をする場合には E/E/PE 開発者との合意が必要である旨の記述	合意した内容は文書化が必要

※「モジュール検証（E/E/PE システム設計＆開発）」の中の “ソフトウェアモジュール仕様書”の参考

項番	参照項番	内容	備考
10.3-4	7.4.5.1	ソフトウェアモジュール設計（ソフトウェアシステム設計）における責任の区分	
10.3-5	7.4.5.4	各ソフトウェアモジュールの設計と各ソフトウェアモジュールに適用される検証内容	IEC61508-3 の TableA.4 参照

※「モジュール検証（E/E/PE システム設計＆開発）」の中の “ソフトウェア妥当性確認計画書”の参考

項番	参照項番	内容	備考
10.2-1	7.3.2.2	・いつ妥当性確認を実施するか ・誰が妥当性確認を実施するか ・ロボットのオペレーションに関連するモード ・ロボットのオペレーションモードの妥当性確認に必要な安全関連ソフトウェア ・妥当性確認のための具体的な戦略 ・妥当性確認を行う環境についての要求事項 ・合否の基準 ・妥当性確認の結果を評価するためのポリシーと手順（特に、異常時について）	妥当性確認のための具体的な戦略については IEC61508-3 Table A.7 を参照
10.2-2	7.3.2.3	次を含んだ安全関連ソフトウェアの妥当性確認の技術的戦略の情報 a)マニュアル又は自動の選択、又はその両方 b)静的又は動的技術の選択、又はその両方 c)分析又は統計技術の選択、又はその両方 d)客観的要因又はエキスパートの判断に基づく合否基準の選択、又は両方	
10.2-3	7.3.2.4	システム安全のソフトウェア側面のための妥当性確認計画の範囲と内容について、評価者又は評価者の代表と同意しなければならない場合の安全度レベル	IEC61508-1 の 8 項参照
10.2-4	7.3.2.5	次についてのソフトウェア妥当性確認の達成のための合否基準 a) 要求される入力信号（そのシーケンスと値を伴ったもの） b) 予測される出力信号（そのシーケンスと値を伴ったもの） c) 他の合否基準（例えばメモリ使用量、タイミング及び許容範囲値	

以下は、実際の運用において必要となる文書（パイロットスタディでは確認しない）

全運用・保全・修理報告書

項番	参照項番	内容	備考
14-1	7.15.2.3	・機能安全監査およびテストの結果 ・E/E/PE 安全関連システムの保全または修理の要請を受けた時期と原因および運用状況 ・E/E/PE 安全関連システムの保全または修理の要請があったときにおける E/E/PE 安全関連システムの性能 ・通常メンテナンス中に見つかった故障の内容 ・ロボット、ロボット制御システム及び E/E/PE 安全関連システムになされた変更内容	運用報告書、保全報告書及び修理報告書は、それらを解析することでインシデントが発見でき得ることがある。（⇒変更要求のエビデンスにつながる）

E/E/PE システム統合試験報告書（H/W）

E/E/PEシステム統合における各種試験の成績書

項番	参照項番	内容	備考
10.4-1	7.5.2.4	テスト結果および設計・開発フェーズで定めた目的と基準を満足しているかどうか	全てのモジュールが意図した機能を実行および意図しない機能が実行されないことを示すこと
10.4-2	7.5.2.4	7.5.2.4 で基準を満足していない（不合格の）場合、その理由と是正措置	
10.4-3	7.5.2.5	統合とテストの間に E/E/PE 安全関連システムの改修や変更があった場合、影響を受けたサブシステムやエレメントの識別	
10.4-4	7.5.2.5	10.4-3 で影響を受けたサブシステムやエレメントの影響解析の結果	
10.4-5	7.5.2.6	統合テストに使用するテスト仕様のバージョン	
10.4-6	7.5.2.6	テストの合格基準	
10.4-7	7.5.2.6	テスト対象の E/E/PE 安全関連システムのバージョン	コンフィグレーション
10.4-8	7.5.2.6	テストに使用するツールと機器（プログラムも含む）	校正データを含む
10.4-9	7.5.2.6	各テスト結果	
10.4-10	7.5.2.6	期待値と実際の結果との全ての不一致	・期待値と実際の結果との比較 ・どのように、どれくらい不一致があったかなど
10.4-11	7.5.2.6	10.4-10 で不一致があった場合、どのような対応を取るか	妥当性確認を続行するか、変更要求を出すか。また、なぜそのように判断したかの理由
10.4.12	7.5.2.7	使用した技術と方策	IEC61508-2 の表 B.3 による

E/E/PE システム検証計画書

E/E/PE システム検証計画書及び検証報告書／記録

項番	参照項番	内容	備考
9-1	7.9.2.1 7.9.2.2 7.9.2.3 7.9.2.4 7.9.2.5 7.9.2.6	E/E/PE 安全関連システム検証計画書 ・全ての基準、技術および使用するツールを記載 ・フェーズにインプットされる基準の正確さと一致を確実にするための活動 ・検証戦略と技術の選定 ・テスト機器の選定と活用 ・検証機器やテストから得られる検証結果の評価 ・各設計と開発フェーズにおいて、機能と安全度の要求事項が満足していることの説明 ・検証活動の結果（検証をパスしたか、故障の理由）	・検証活動の結果については次を考慮 - E/E/PE システム安全ライフサイクルの1つ以上の関連する要求事項に合わないアイテム - 1つ以上の関連する設計基準に合わないアイテム - 1つ以上の関連する安全マネジメント要求事項に合わないアイテム
9-2	7.9.2.7	E/E/PEシステム設計要求事項がE/E/PEシステム安全要求仕様書を十分満足しているかどうか	E/E/PE システム設計と開発の開始前に検証
9-3	7.9.2.8	・E/E/PE システム設計と開発のための E/E/PE システムテストが十分かどうか ・E/E/PE システム安全要求事項と E/E/PE システム設計と開発との度性と完全性	・E/E/PE システム統合の開始前に検証 ・検証ための故障分析やテスト技術は IEC61508-2 の TableB.5 が推奨される
9-4	7.9.2.9	E/E/PEシステム設計要求事項がE/E/PEシステム安全要求仕様書を満足していることの確認	
9-5	7.9.2.10	E/E/PE システム統合検証のテストケースと結果	

＜以下参考＞

共通の手順書など

共通の手順書など（例）		
基準	文書（例）	内容
文書管理	文書番号付与規定	文書番号のつけ方を示した規定
文書管理	文書管理規定	文書の名称、責任部署、改定、保管、など文書管理に関する決まり
品質管理	検査検定基準	部品調達、設計、生産時の検証、検査などを示した基準 報告書の様式なども含む
品質管理	市場品質基準	市場での不具合の取り扱い、クレームの取り扱いに関する規定、それらの設計変更基準との連携
品質管理	測定器校正規定	設計、開発を含み、検証、検査、生産などに用いられる測定器の校正を規定した書類
品質規定	内部監査規定	品質や工程の内部監査に関する規定。機能安全評価に関する記述を含むこと。
人事管理	教育訓練規定	社員の教育訓練を規定した文書。教育訓練記録の保管などに関する要求も含む
人事管理	職務能力規定	設計開発、品質管理部門を含む　職務ごとに要求される能力を示した書類。
人事管理	職務分掌規定	技術、開発、品質管理部門を含む各組織の職務内容や責任範囲を示した文書。
人事管理	組織図	技術、開発、品質管理部門を含む各組織およびそれらの関係を示した文書。
技術管理	コーディング標準	ソフトウェアのコーディング標準を示した決まり
技術管理	設計開発基準	各段階での必要書類などの記述を含み、設計手順や設計工程を規定した基準 デザインレビューや、各設計段階での検証に関する記述 検証や、解析に用いる手法の選定基準などに関する規定 計画、報告書、記録の作成、保管等に関する規定 V モデル以外は、その工程の正当性を示す内容を含むこと
技術管理	設計変更基準	設計変更の手順を示した規定 必要な様式や、変更の妥当性を確認する委員会、影響解析の必要性の判断基準などを含む

製品のライフサイクルに関連するもの

安全ライフサイクル			文書(例)	内容
1	IEC61508-1 7.2 項 (Box 1)	コンセプト	製品概要書	開発する製品のコンセプトを述べた書類
2	IEC61508-1 7.3 項 (Box 2)	全体の範囲決定	対象範囲説明書	製品がカバーする範囲を規定する書類。製品企画書に含まれる場合もある。外部安全方策に依存する場合は、その境界を明確にすること。
3	IEC61508-1 7.4 項 (Box 3)	危害と危険の解析	リスクアセスメントレポート	リスクアセスメントのレポート
4	IEC61508-1 7.5 項 (Box 4)	全体の安全要求	全安全要求仕様書	全体の安全要求を示した仕様書
5	IEC61508-1 7.6 項 (Box 5)	全体の安全配置	全安全要求配置書	安全要求の配置を述べた書類。例えば、「どの入力部分にどんな機能を割り当てるか」といった文書。
6	IEC61508-1 7.7 項 (Box 6)	全体の運用と保全計画	運用保全計画書	システム全体の運用と保全計画を記載した文書。
7	IEC61508-1 7.8 項 (Box 7)	全体の安全妥当性確認計画	全安全妥当性確認計画書	システム全体の安全妥当性確認計画。いつどのような試験や評価を行うかなどを具体的に記入。
8	IEC61508-1 7.9 項 (Box 8)	全体の据付・立ち上げ計画	据付・立上げ計画書	設置及び立ち上げに関する計画。いつどのように、どんな順番で据付、立ち上げを行うかの具体的な計画。
9	IEC61508-2 7.2 項 (Box 10.2)	E/E/PE 系安全要求仕様	E/E/PE システム安全要求仕様書	システムの安全機能や安全度を規定する仕様書。多くのサブシステムや、エレメントの仕様書もここに含まれるかもしれない。
10		E/E/PE 安全関連系実現化	安全関連システム実現化	
12	IEC61508-1 7.13 項 (Box 12)	全体の据付と立ち上げ	据付・立上げ報告書	設置や立ち上げの報告書。問題があれば、適切なライフサイクルフェーズに戻すための充分な情報を含むこと。
13	IEC61508-1 7.14 項 (Box 13)	全体の安全妥当性確認	全安全妥当性確認報告書／記録	妥当性確認試験の報告書。問題があれば、適切なライフサイクルフェーズに戻すための充分な情報を含むこと。
14	IEC61508-1 7.15 項 (Box 14)	全体の運用、保全、修理	全運用・保全・修理記録	システムの運用、保全および修理記録
15	IEC61508-1 7.16 項 (Box 15)	全体の変更と改造	全変更・改造要求書	変更要求の書類
			全変更・改造報告書／記録	変更履歴の記録
16	IEC61508-1 7.17 項 (Box 16)	運用停止や廃棄	運転停止・廃棄報告書	廃棄要求、廃棄計画書、廃棄の記録
全てのフェーズに関して		計画、実行、報告、記録の文書化が確実に行われること。文書は、開発の進行に伴い必要な改定がなされること。		

E/E/PE 系安全ライフサイクル（ハード）

E/E/PE 系安全ライフサイクルフェーズ		文書(例)	内容
E/E/PE 系妥当性確認計画	IEC61508-2 7.3 項（Box 10.2）	E/E/PE 系妥当性確認計画書	E/E/PE システムの妥当性確認計画を示した書類。確認時期、内容、方法、測定器など妥当性確認に必要な情報を記載。
E/E/PE 系設計と開発 E/E/PE 系構造		システムブロック図 システム統合試験指示書	以下の内容を含む、システムの構造を示す書類: ハードウェアやソフトウェアに関する E/E/PE システムの構造設計の記述 プログラマブル機器の統合試験の仕様 プログラマブルとそうでないハードウェアの統合試験の仕様
E/E/PE 系設計と開発 ハードウェアの構造		ハードウェア仕様書 ブロック図 統合試験指示書	ハードウェア構造設計仕様と、ハードウェア構造の統合試験仕様
E/E/PE 系設計と開発 ハードウェアモジュール設計		モジュール仕様書 回路図 部品表 試験指示書	ハードウェアモジュール設計仕様と、ハードウェアモジュール試験仕様
E/E/PE 系設計と開発 コンポーネントの構造や調達		購入部品の仕様書・構造図 購入部品の試験報告書	購入部品の性能や使い方、試験結果や正しい使用方法が分かる書類
プログラマブル機器統合	IEC61508-2 7.5 項（Box 10.4）	プログラマブル機器統合試験レポート	モジュールやサブシステムレベルでの、プログラマブル機器のハードとソフトの統合試験報告書。試験仕様書に基づき行った試験結果を示すこと。
E/E/PE 機器システム統合	IEC61508-2 7.5 項（Box 10.4）	部分統合試験レポート	E/E/PE 機器に対して行った統合試験の報告書。試験仕様書に基づき行った試験結果を示すこと。
E/E/PE 機器運用と保全手順	IEC61508-2 7.6 項（Box 10.5）	ユーザーマニュアル サービスマニュアル	ユーザー向け取扱説明書、 運用者、保全者向けマニュアル(運用マニュアル、サービスマニュアル）
E/E/PE 系安全妥当性確認	IEC61508-2 7.7 項（Box 10.6）	統合妥当性確認レポート	システム全体に対して行った妥当性確認の報告書。仕様書に基づき行った結果を示すこと。トレーサビリティー確保のために必要な情報の記載があること。
E/E/PE システム変更	IEC61508-2 7.8 項	E/E/PE システムの変更手順書	（共通の手順書の表を参照）
		変更要求書	変更が必要になった理由や、変更内容などの記述
		影響解析レポート	変更が及ぼす影響を記載した報告書
		変更記録	変更の実施など変更履歴を記載した記録
全てのフェーズに関して	計画、実行、報告、記録の文書化が確実に行われること。文書は、開発の進行に伴い必要な改定がなされること。必要事項が安全マニュアルに反映されること。		

ソフトウェア安全ライフサイクル

ソフトウェア安全ライフサイクルフェーズ			文書(例)	内容
ソフトウェア安全要求			ソフトウェア安全仕様書	ソフトウェアの安全機能要求とソフトウェアの安全度要求を記述したソフトウェア安全要求仕様書
ソフトウェア妥当性確認計画		IEC61508-3 7.3 項（Box10.2）	ソフトウェア安全妥当性確認計画書	ソフトウェア安全仕様書への適合確認を行う計画を書いた書類。試験時期、試験方法、必要な試験装置や環境などの記載があること。
ソフトウェア設計・開発	ソフトウェア構造		ソフトウェア構造仕様書	ソフトウェア構造設計に関する記述、ソフトウェア構造統合試験仕様書、プログラマブルなハードウェアとソフトウェアの統合試験仕様、開発ツールやコーディングマニュアルに関する記述
	ソフトウェアシステム設計		ソフトウェアシステム仕様書	ソフトウェア設計に関する記述、ソフトウェアシステム統合試験計画及び仕様書
	ソフトウェアモジュール設計		ソフトウェアモジュール仕様書	ソフトウェアモジュール設計仕様書、ソフトウェアモジュール試験計画及び仕様書
	コーディング		ソースコードのリスト	モジュールごとに作られたソースコードのリスト
			コードレビュー結果報告書	各ソースコードのコードレビューの結果が書かれた報告書
	ソフトウェアモジュール試験		ソフトウェアモジュール試験報告書	各ソフトウェアモジュールの試験報告書。トレーサビリティー確保のための情報を有すること。
	ソフトウェア統合		ソフトウェアモジュール統合試験報告書	エレメントレベルでの統合試験報告書
			ソフトウェアシステム統合試験報告書	サブシステムレベルでの統合試験報告書
			ソフトウェア構造統合試験報告書	システムレベルでの統合試験報告書
プログラマブル機器統合		IEC61508-3 7.5 項（Box 10.4）	組み込み評価試験報告書	プログラマブルなハードウェアに組み込んで行った試験結果の報告書
ソフトウェア運用と保全手順		IEC61508-3 7.6 項（Box 10.5）	ユーザーマニュアル	ユーザー向けの取扱説明書
			サービスマニュアル	保全及びサービス向けの説明書
ソフトウェア安全妥当性確認		IEC61508-3 7.7 項（Box 10.6）	ソフトウェア安全妥当性確認試験報告書	システム全体に関してソフトウェアがその仕様に適合していることの確認を行った試験報告書。
ソフトウェア変更		IEC61508-3 7.8 項	ソフトウェア変更手順書	(共通の手順書の表を参照)
			ソフトウェア変更申請書	ソフトウェアの変更が必要になった理由や、変更内容などの記載
			ソフトウェア変更影響解析報告書	ソフトウェアの変更がもたらす影響を解析した報告書。
			ソフトウェア変更履歴	ソフトウェアの変更履歴
全フェーズに関して		計画、実行、報告、記録の文書化が確実に行われること。文書は、開発の進行に伴い必要な改定がなされること。必要事項が安全マニュアルに反映されること。		